SF-APP:
A Secure Framework for Authentication and Privacy Preservation in Opportunistic Networks

Prashant Kumar, National Institute of Technology Hamirpur, India
Naveen Chauhan, National Institute of Technology Hamirpur, India
Narottam Chand, National Institute of Technology Hamirpur, India
Lalit K. Awasthi, Dr. B. R. Ambedkar National Institute of Technology, Jalandhar, India

ABSTRACT

Opportunistic networks are the special class of ad hoc networks where permanent link among the nodes are almost absent and communication occurs when an “opportunity” is found. The opportunistic networks have more diverse features than traditional ad hoc networks, like self-organized nature, intermittent connectivity, store-carry-forward routing mechanism, etc. All these features make opportunistic networks more prone to security threats. This article discusses security challenges and threats to opportunistic networks. Focusing on the specific security requirements of opportunistic networks, proposed is a secure framework for authentication and privacy preservation (SF-APP) for opportunistic networks. The proposed algorithm takes care of authentication, privacy preservation, and trust management. Within this article is a performed security analysis of SF-APP and simulation results show that the proposed framework is capable of fulfilling the security requirements of opportunistic networks.

KEYWORDS
Delay Tolerant Networks, Opportunistic Networks, Privacy, Security, Security Framework, Trust Management

INTRODUCTION

Opportunistic networks (OppNets) have evolved as a special class of mobile ad-hoc and delay tolerant networks which have a vast range of applications including disaster and rescue networks (Lilien, Gupta, & Yang, 2007), wildlife monitoring (Sadler & Martonosi, 2004), social networking DakNet (Pentland, Fletcher, & Hasson, 2004), PodNet (“PodNet - Mobile Distribution of User-generated Content [PodNet Project],” n.d.), Haggle (Nordström, Rohner, & Gunningberg, 2014) to name a few. In OppNets, end-to-end connectivity among the nodes is absent. OppNets use receive-carry-forward routing mechanism instead of receive-forward (W. Wang, Guo, Zheng, Tang, & Wang, 2015). Due to diverse features, such as intermittent connectivity, seed deployment, different routing mechanism, mobility, delay tolerant nature, OppNets have many security concerns. Security solutions designed
for traditional wireless and ad-hoc networks cannot be directly applied to OppNets, as they have different unique features.

A variety of communication technologies are used in OppNets. These devices may vary in communication, computational and energy resources. Mobility and frequent link disruption make OppNets topology even more dynamic and flexible. In OppNets no direct path exists between the source and destination. So, the nodes have to hold the data with themselves till the next communication opportunity is found. Thus, the data moves closer to destination hop by hop. Hence trust becomes very important as if any node behaves maliciously then network performance may be degraded by a huge factor. Even whole network can be disrupted, since the malicious node can temper with the original message or can replace the whole message by putting bogus/wrong information. Due to various factors discussed and adaptive nature, it is crucial to provide good privacy and security in opportunistic network, not only for the classical use cases but also when considering emerging application paradigms such as mobile sensing and opportunistic computing (Trifunovic et al., 2017). Additionally, user privacy is another important issue in OppNets, as users own their personal devices. Since many routing protocols use context information; this may be sensitive to some users. This implies the necessity of a security solution which can cope up with the specific requirements of OppNets.

In this paper, we addressed these issues and proposed an authentication and incentive based secure framework that prevents unauthorized users from accessing sensitive information, maintains the confidentiality of data, preserves the privacy of users and helps to develop trust among the users. Our proposed framework (SF-APP) has the mechanism for authentication, privacy preservation and trust management. The design objectives of SF-APP are:

1. To design an authentication and encryption mechanism that prevent the unauthorized users from accessing the vital information as well as ensure the confidentiality and integrity of data;
2. To design an incentive scheme that gives the special benefits to the legitimate users and helps to develop the trust among the users.

The main contributions of this paper are:

1. Proposed secure framework SF-APP (Secure Framework for Authentication and Privacy Preservation);
2. Authentication using dynamic IDs;
3. Trust based forwarding mechanism;

**OPPORTUNISTIC NETWORK SECURITY**

In this section, we described specific challenges, threats and security requirements and threats concerned with OppNets.

**Challenges**

An OppNets grows from its seed, by extending invitations to join the networks to other devices that are available (Lilien, Kamal, Bhuse, & Gupta, 2006). As per the network requirement, these nodes self-localize and self-configure them. Nodes are mobile and free to join/leave the network without any prior information. Thus, scalability becomes another issue. With the scarcity of resources, it is challenging to ensure the communication opportunity in dynamic and heterogeneous networks. OppNets use store-carry-forward routing mechanism. This mechanism is helpful to extend the connectivity and to improve the data delivery. Devices involved in the OppNets are equipped with different radio interfaces that vary from Bluetooth, Wi-Fi, Satellite, WiMAX to 4G-LTE. These devices have significant variation in transmission and receiving capabilities (Chlamtac & Lerner,
A Critical Review of the Big-Data Paradigm
www.igi-global.com/chapter/a-critical-review-of-the-big-data-paradigm/217823?camid=4v1a

An Adapted Ant-Inspired Algorithm for Enhancing Web Service Composition
www.igi-global.com/chapter/an-adapted-ant-inspired-algorithm-for-enhancing-web-service-composition/217869?camid=4v1a